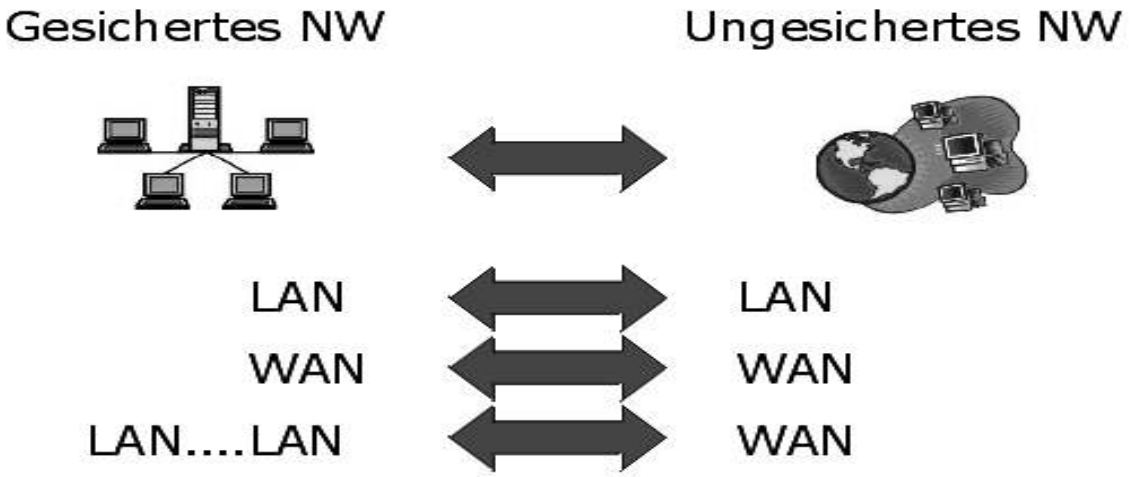
Erkennung und Verhinderung von Netzangriffen

1. Firewall
2. IDS
3. AAA-Dienste

1. Firewall

- Analogie: elektronischer Pförtner + elektr. Brandschutzmauer
- Sicherung u. Kontrolle zw. zu schützendem - und öffentlichem Netz
- zwei wesentliche Aufgaben:
  - Gefahrenabwehr
  - Zugangs- und Ausgangskontrolle (Identifikation, Authentifikation)



Allgemeine Ziele von Firewall-Systemen:

- Zugangskontrolle auf Netzwerkebene
- Zugangskontrolle auf Benutzerebene
- Zugangskontrolle auf Datenebene
- Rechteverwaltung
- Kontrolle auf der Anwendungsebene
- Entkoppelung von Diensten
- Beweissicherung und Protokollauswertung
- Alarmierung
- Verbergen der internen Netzstruktur
- Vertraulichkeit von Nachrichten

Unterscheidung in 3 Arten von Zugriffskontrollsystemen:

- Paketfilter

  Filterung basierend auf Sicherungs- und Vermittlungsschicht

2. Circuit-Relays

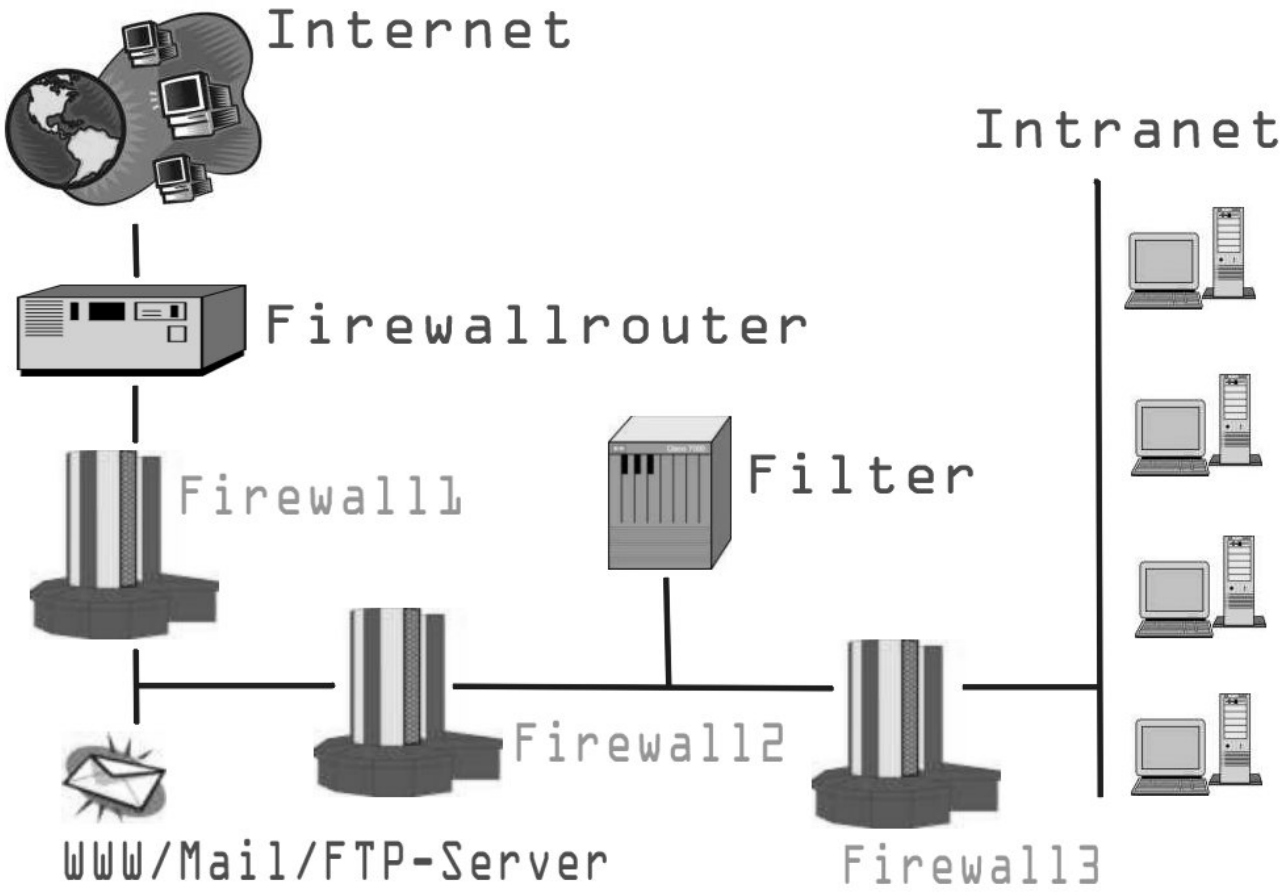
   Keine direkte Verbindung nach außen aufbaubar

3. Application Gateways

   Jede Verbindung wird auf ihre Zulässigkeit überprüft

Zunahme der Sicherheit

Mögliches Firewall-Konzept:



2. IDS (Intrusion Detection System)

•Definition:

Ein System, dass versucht, eine Intrusion automatisch zu erkennen, und Daten zur Verfügung stellt, die eine manuelle und/oder automatische Antwort auf diesen Verstoß ermöglichen.

- Ergänzung des Sicherheitssystems
- Einsatz auf beiden Seiten der Firewall
  → Erkennung von Angriffsversuchen sowohl aus dem Netz als auch von innen (Viren, trojanische Pferde)

Abgrenzung

IDS ←→ Firewall, Filtering, Proxies

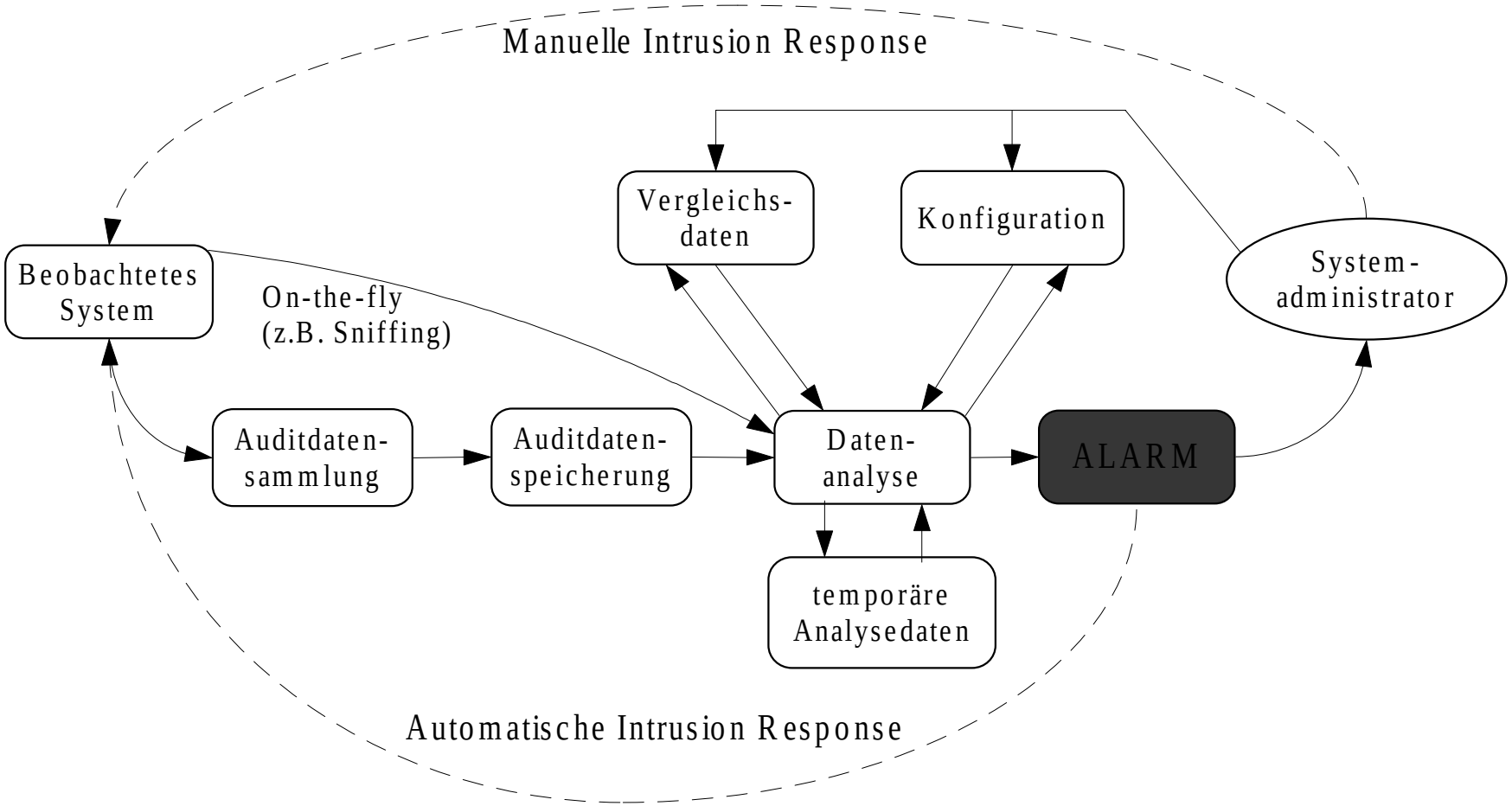
- Die rechts stehenden Komponenten sind nur Torwächter. Zudem hat das Tor definierte Einlässe.
- Falls diese Einlässe kompromittiert werden oder der Wächter überwunden wird, kann ein IDS dies erkennen.
- Ein IDS kann auch das Innere eines Netzes überwachen.
- IDS sollten zusätzlich eingesetzt werden.

Grundlegender Aufbau eines IDS

IDS bestehen aus drei Hauptkomponenten:

- Komponente zur Datensammlung
  - Informationen über den aktuellen Systemzustand und die Betriebsmittelvergabe.
- Komponente zur Datenanalyse
  - Analyse in Hinblick auf mögliche Angriffe.
- Komponente zur Ergebnisdarstellung
  - Alarmierung per Email, Pager oder gesicherten Netzkanal.

Verallgemeinerte Konzeptskizze



3. AAA-Dienste

Schutz des Rechners vor Netzangriffen durch Zugriffskontrolle – AAA:

- Authentication(Identität feststellen)
Bereitstellung der Feststellung der Personalität eines Benutzers, Rechners oder einer Netzkopplungselemente bzw. eines Subjekts der Datensicherheitspolitik

- Authorization (Zugriffsrechte prüfen)
Definierung der Services, die konkretem Subjekt der Datensicherheitspolitik geeignet sind Cisco Systems - Weltleader im Bereich von Kopplingselementen für LANs und WANs

3. AAA-Dienste

-Accounting (Aufzeichnen)
Bereitstellung der Sammlung, Analyse und Verteilung der Information über die Services, die konkretem Subjekt der Datensicherheitspolitik geeignet sind

Authentication Authorization Accounting

Fazit:

- Es gibt viele Möglichkeiten Rechnernetzwerke vor möglichen Netzangriffen zu schützen
- Guten Schutz bieten die drei genannten Möglichkeiten in der Kombination
- Die Datenbanken der Elemente sollten regelmäßig aktualisiert werden